Techniques d'attaques laser appliquées à la rétro-conception de mémoires

Description

Les systèmes numériques sont désormais profondément intégrés dans notre quotidien et essentiels au fonctionnement de notre société. Dans ces systèmes, les mémoires jouent un rôle crucial dans le stockage et la manipulation des secrets, tels que les clés cryptographiques, les programmes de démarrage (*bootloader*) ou encore les codes propriétaires. C'est aussi via les mémoires que sont stockés les options de configuration, comme les modes de débogage et les privilèges d'accès. Une grande variété de mémoires existe : les mémoires non volatiles (NVM), comme la FLASH, ou la MRAM, les FUSES, ROM. Et les mémoires non volatiles comme la SRAM, la DRAM. Pour garantir la sécurité des systèmes, il est impératif de comprendre l'organisation des mémoires et de maîtriser les méthodes d'attaque à l'état de l'art pour extraire ou modifier leur contenu.

L'objectif principal de cette thèse est l'étude de la sécurité des mémoires vis-à-vis des perturbations laser. Les attaques par injections de fautes laser sont connues depuis le début des années 2000 [1] et désormais largement mises en œuvre dans les caractérisations sécuritaires et les schémas d'évaluations. L'effet des fautes sur les mémoires volatiles [2] ou non [3] a été largement étudiés. Cette thèse va aborder le problème sous l'angle de la rétro-conception en se posant la question : comment les injections laser peuvent être utilisées pour retrouver l'organisation d'une mémoire et en extraire et/ou modifier le contenu.

Un premier axe de travail étudiera les approches dites par « Thermal Laser Stimulation» (TLS), qui permettent d'extraire de l'information de manière passive d'une mémoire. Par rapport aux études existantes [4], nous étudierons l'effet du type de nœud technologique et de sa taille. Nous chercherons notamment à déterminer si la précision est suffisante pour mettre en place les attaques TLS sur une technologie 22nm FDSOI.

Un second axe de travail sera d'utiliser les techniques laser pour la rétro-conception d'une architecture mémoire. Il s'agira notamment : d'aider à comprendre l'organisation des données, trouver les paramètres d'éventuels codes détecteurs/correcteurs d'erreurs. Plus généralement aider à la compréhension de la mémoire, en analyses préliminaires à d'autres techniques d'analyses plus spécifiques.

Informations Pratiques

Le doctorat aura lieu au CEA-LETI en France, à Grenoble, au sein du Laboratoire de Tests de Sécurité et Outils (LTSO). Le LTSO est une équipe d'environ 15 experts en sécurité et plusieurs doctorants. Le laboratoire est spécialisé dans les tests de sécurité des produits et le développement d'outils pour la recherche sur les vulnérabilités. Le laboratoire dispose notamment d'équipements à l'état de l'art pour l'injection de fautes laser et le TLS qui seront utilisés tout au long du travail de doctorat.

Le doctorat sera encadrée par Thomas Hiscock, Simon Pontié, Maxime Lecomte et dirigé par Jessy Cledière.

Date de début : Septembre-Décembre 2025

Si vous êtes intéressé, veuillez envoyer votre CV à Thomas Hiscock (thomas.hiscock@cea.fr) et (jessy.clediere@cea.fr)

Bibliographie

[1] S. P. Skorobogatov and R. J. Anderson, "Optical Fault Induction Attacks," in *Cryptographic Hardware and Embedded Systems - CHES 2002*, B. S. Kaliski, çetin K. Koç, and C. Paar, Eds., Berlin, Heidelberg: Springer, 2003, pp. 2–12. doi: 10.1007/3-540-36400-5_2.

[2] A. Sarafianos, C. Roscian, J.-M. Dutertre, M. Lisart, and A. Tria, "Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an SRAM cell," *Microelectronics Reliability*, vol. 53, no. 9, pp. 1300–1305, Sep. 2013, doi: 10.1016/j.microrel.2013.07.125.

[3] B. Colombier, A. Menu, J.-M. Dutertre, P.-A. Moëllic, J.-B. Rigaud, and J.-L. Danger, "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller," in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2019, pp. 1–10. doi: 10.1109/HST.2019.8741030.

[4] H. Lohrke, S. Tajik, T. Krachenfels, C. Boit, and J.-P. Seifert, "Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 573–595, Aug. 2018, doi: 10.13154/tches.v2018.i3.573-595.